IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS
EASTERN DIVISION

SERGEI STADNIK, on behalf of himself and all others similarly situated, Plaintiff, v. **SOVOS COMPLIANCE, LLC,** Defendant.	**Case No.** **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Sergei Stadnik ("Plaintiff"), individually and on behalf of all similarly situated persons, alleges the following against Sovos Compliance, LLC, ("Sovos" or "Defendant") based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by Plaintiff's counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiff brings this class action against Sovos for its failure to properly secure and safeguard Plaintiff's and other similarly situated individuals' names, dates of birth, Social Security numbers, and account numbers (the "Private Information" or "PII") from hackers.

2. Sovos, which is based in Wilmington, Massachusetts, is a digital regulatory compliance company. As part of its business, and in order to earn profits, Defendant obtained and stored the Private Information of Plaintiff and Class Members.

3. On or about July 13, 2023, Sovos filed its first of three official notices of data security incident with the Maine Attorney General, followed by another notice on August 23, 2023, and September 5, 2023.

4. On or about August 30, 2023, Sovos also sent out data breach notice letters (the "Notice") to individuals whose Private Information was compromised as a result of the cyber attack.

5. Based on the Notice, Sovos detected unusual activity on some of its computer systems on or around May 31, 2023. In response, Defendant "took the affected application offline", launched an investigation, and notified law enforcment. Defendant's investigation revealed that unauthorized third parties had accessed certain files that contained sensitive clients' customer's information ("the Data Breach").

6. At the time of this filing, Defendant has not disclosed how long the unauthorized users had access to Plaintiff's and approximately 215,114 other individuals highly sensitive private information stored on Defendant's systems.

7. As a result of Defendant's inability to timely detect the Data Breach, Plaintiff and "Class Members" (defined below) had no idea for more than two (2) months that their Private Information had been compromised, and that they were at significant risk of experiencing identity theft and various other forms of personal, social, and financial harm. This substantial and imminet risk will remain for their respective lifetimes.

8. The Private Information compromised in the Data Breach included highly sensitive data that represents a gold mine for data thieves, including but not limited to, customers' names, dates of birth, Social Security numbers, and account numbers that Sovos collected and maintained from its clients.

9. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

10. There has been no assurance offered by Defendant that all personal data or copies of data have been recovered or destroyed, or that Defendant has adequately enhanced its data security practices sufficient to avoid a similar breach of its network in the future.

11. Therefore, Plaintiff and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

12. Plaintiff brings this class action lawsuit to address Sovos's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and its failure to timely detect the Data Breach.

13. The potential for improper disclosure and theft of Plaintiff's and Class Members' Private Information was a known risk to Sovos, and thus it was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

14. Upon information and belief, Sovos failed to properly monitor its systems and implement adequate data security practices with regard such systems that housed the Private

Information. Had Sovos properly monitored its network systems and implemented such practices, it could have prevented the Data Breach or at least discovered it sooner.

15. Plaintiff's and Class Members' identities are now at risk because of Sovos's negligent conduct as the Private Information that Sovos collected and maintained is now in the hands of data thieves and other unauthorized third-parties.

16. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed and compromised during the Data Breach.

17. Accordingly, Plaintiff, on behalf of himself and the Class, asserts claims for negligence, negligence per se, breach of third-party beneficiary contract, unjust enrichment, and declaratory and injunctive relief.

II. PARTIES

18. Plaintiff Sergei Stadnik is, and at all times mentioned herein was, an individual citizen of the State of Arizona.

19. Defendant Sovos, Inc., is a global digital regulatory compliance organization incoprated in Wilmington, with its principal place of business at 200 Ballardvale Street, building 1, 4th floor, Wilmingon, Massachusetts, 01887 in Middlesex County.

III. JURISDICTION AND VENUE

20. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from Sovos. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

21. This Court has jurisdiction over Sovos because Sovos operates in and/or is incorporated in this District.

22. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and Sovos has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Sovos's Business and Collection of Plaintiff's and Class Members' Private Information

23. Sovos is a digital regulatory compliance company. Founded in 1979, Sovos works in connection with its clients to regulate and maintain customer accounts. Sovos employs more than 2,600 people and generates approximately $504 million in annual revenue.

24. As a condition of providing regulatory compliance services, Sovos requires that its clients entrust it with highly sensitive customer PII, including that of Plaintiff and Class Members.

25. In its "Privacy Policy," Sovos claims that "Protecting consumer privacy is important" and informs clients and its clients' customers that:

> Sovos shall take reasonable steps to protect the Information from loss, misuse and unauthorized access, disclosure, alteration and destruction. Sovos has put in place appropriate physical, electronic and managerial procedures to safeguard and secure the Information from loss, misuse, unauthorized access or disclosure, alteration or destruction.[1]

26. Sovos uses this information, inter alia, for marketing and sales purposes.

27. Because of the highly sensitive and personal nature of the information Sovos acquires and stores with respect to its clients' current and former customers, Sovos, upon information and belief, promises to, among other things: keep its clients' current and former

[1] *See* https://sovos.com/privacy-policy/ (last visited Sept. 12, 2023).

customers' Private Information private; comply with industry standards related to data security and the maintenance of its clients' customers' Private Information; inform its clients (and their customers) of its legal duties relating to data security and comply with all federal and state laws protecting its clients' customers' Private Information; only use and release its clients' customers' Private Information for reasons that relate to the services it provides; and provide adequate notice to its clients' customers if their Private Information is disclosed without authorization.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Sovos assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from unauthorized disclosure and exfiltration.

29. Plaintiff and Class Members and their respective institutions relied on Sovos to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach and Sovos's Inadequate Notice to Plaintiff and Class Members

30. According to Defendant's Notice, it learned of unauthorized access to its computer systems on May 31, 2023, with such unauthorized access having taken place on an undisclosed date.

31. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including Plaintiff's and Class Members' Social Security numbers and account numbers.

32. On or about August 30, 2023, Sovos finally began to notify the majority of impacted individuals that its investigation deterimined that their Private Information was compromised.

33. Sovos delivered the Notice to Plaintiff and Class Members, alerting them that their highly sensitive Private Information had been exposed in a "security event."

34. The notice letter then attached additional pages that listed time-consuming steps that victims of data security incidents can take to mitigate the inevitable negative impacts of the Data Breach on their lives, such as getting a copy of a credit report, reviewing account statements, placing freezes on their credit, and/or notifying law enforcement about suspicious financial account activity.

35. Other than providing only two years of crediting monitoring that Plaintiff and Class Members would have to affirmatively sign up for, along with a call center number that victims could contact with questions, Sovos offered no other substantive steps to help victims like Plaintiff and Class Members to protect themselves. On information and belief, Sovos sent a similar generic letter to all individuals affected by the Data Breach.

36. Sovos had obligations created by contract, industry standards, and common law to keep Plaintiff's and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

37. Plaintiff and Class Members provided their Private Information to Sovos's clients with the reasonable expectation and mutual understanding that Sovos would comply with its obligations to keep such information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

38. Sovos's data security obligations were particularly important given the substantial increase in cyberattacks in recent years. Sovos knew or should have known that its electronic records would be targeted by cybercriminals. However, even with these obligations and this knowledge, it failed to safeguard the Private Information.

C. Sovos Failed to Comply with FTC Guidelines

39. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decisionmaking. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

40. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

41. The FTC further recommends that companies not maintain personally identifiable information ("PII") longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

42. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data by treating the failure to employ reasonable and

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

43. As evidenced by the Data Breach, Sovos failed to properly implement basic data security practices. Sovos's failure to employ reasonable and appropriate measures to protect against unauthorized access to and exfiltration of Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

44. Sovos was at all times fully aware of its obligation to protect the Private Information of its customers yet failed to comply with such obligations. Defendant was also aware of the significant repercussions that would result from its failure to do so.

D. Sovos Failed to Comply with Industry Standards

45. As noted above, experts studying cybersecurity routinely identify businesses like Sovos as being particularly vulnerable to cyberattacks because of the value and volume of the Private Information which they collect and maintain.

46. Some industry best practices that should be implemented by these companies, including Sovos, are, without limitation: educating all employees and implementing strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, and multi-factor authentication, as well as backing up data and limiting which employees can access sensitive data.

47. As evidenced by the Data Breach, Defendant failed to follow some or all of these industry best practices.

48. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as

firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

49. As evidenced by the Data Breach, Defendant also failed to follow these cybersecurity best practices.

50. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

51. Defendant failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

E. Sovos Breached its Duty to Safeguard Plaintiff's and Class Members' Private Information

52. In addition to its obligations under federal and state law, Sovos owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Sovos owed a duty to Plaintiff and Class Members to provide reasonable security, including complying with industry standards and requirements, training for its staff, and ensuring that its computer systems, networks, and protocols adequately protected the Private Information of Plaintiff and Class Members.

53. Sovos breached its obligations to Plaintiff and Class Members and was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems

and data. Sovos's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect its clients' customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of its clients' customers' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiff's and Class Members' Private Information.

54. Sovos negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

55. Had Sovos remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, it could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Private Information.

56. Accordingly, Plaintiff's and Class Members' lives have been severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft.

F. Sovos Should Have Known that Cybercriminals Target Highly Sensitive PII to Carry Out Fraud and Identity Theft

57. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiff and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[2] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

58. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

59. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired

[2] *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Sept. 12, 2023).

information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

60. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

61. Thus, even if certain information was not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiff's and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiff and Class Members.

62. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps (similar to those suggested by Defendant in its Notice) to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[3] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

63. Identity thieves can also use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud,

[3] *See IdentityTheft.gov*, Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Sept. 12, 2023).

to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

64. PII is data that can be used to detect a specific individual. PII is a valuable property right. Its value is axiomatic, considering the value of big data in corporate America and the consequences of cyber thefts (which include heavy prison sentences). Even this obvious risk-to-reward analysis illustrates beyond doubt that PII has considerable market value.

65. The U.S. Attorney General stated in 2020 that consumers' sensitive personal information commonly stolen in data breaches "has economic value."[4] The increase in cyberattacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendant's industry.

66. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, PII can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[5] Experian reports that a stolen credit or debit card number can

[4] *See Attorney General William P. Barr Announces Indictment of Four Members of China's Military for Hacking into Equifax*, U.S. Dep't of Justice, Feb. 10, 2020, available at https://www.justice.gov/opa/speech/attorney-general-william-p-barr-announces-indictment-fourmembers-china-s-military (last visited on Sept. 12, 2023).

[5] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited on Sept. 12, 2023).

sell for $5 to $110 on the dark web and that the "*fullz*" (a term criminals who steal credit card information use to refer to a complete set of information on a fraud victim) sold for $30 in 2017.[6]

67. Furthermore, even information such as names, email addresses and phone numbers, can have value to a hacker. Beyond things like spamming customers, or launching phishing attacks using their names and emails, hackers, *inter alia*, can combine this information with other hacked data to build a more complete picture of an individual. It is often this type of piecing together of a puzzle that allows hackers to successfully do phishing attacks or social engineering attacks. This is reflected in recent reports, which warn that "[e]mail addresses are extremely valuable to threat actors who use them as part of their threat campaigns to compromise accounts and send phishing emails."[7]

68. The Dark Web Price Index of 2022, published by PrivacyAffairs[8] shows how valuable just email addresses alone can be, even when not associated with a financial account:

Email Database Dumps	**Avg. Price USD (2022)**
10,000,000 USA email addresses	$120
600,000 New Zealand email addresses	$110
2,400,000 million Canada email addresses	$100

69. Beyond using email addresses for hacking, the sale of a batch of illegally obtained email addresses can lead to increased spam emails. If an email address is swamped with spam, that address may become cumbersome or impossible to use, making it less valuable to its owner.

---

[6] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited on Sept. 12, 2023).

[7] *See* https://www.magicspam.com/blog/dark-web-price-index-the-cost-of-email-data/ (last visited on Sept. 12, 2023).

[8] *See* https://www.privacyaffairs.com/dark-web-price-index-2022/ (last visited on Sept. 12, 2023).

70. Likewise, the value of PII is increasingly evident in our digital economy. Many companies collect PII for purposes of data analytics and marketing. These companies, collect it to better target customers, and shares it with third parties for similar purposes.[9]

71. One author has noted: "Due, in part, to the use of PII in marketing decisions, commentators are conceptualizing PII as a commodity. Individual data points have concrete value, which can be traded on what is becoming a burgeoning market for PII."[10]

72. Consumers also recognize the value of their personal information, and offer it in exchange for goods and services. The value of PII can be derived not only by a price at which consumers or hackers actually seek to sell it, but rather in the economic benefit consumers derive from being able to use it and control the use of it.

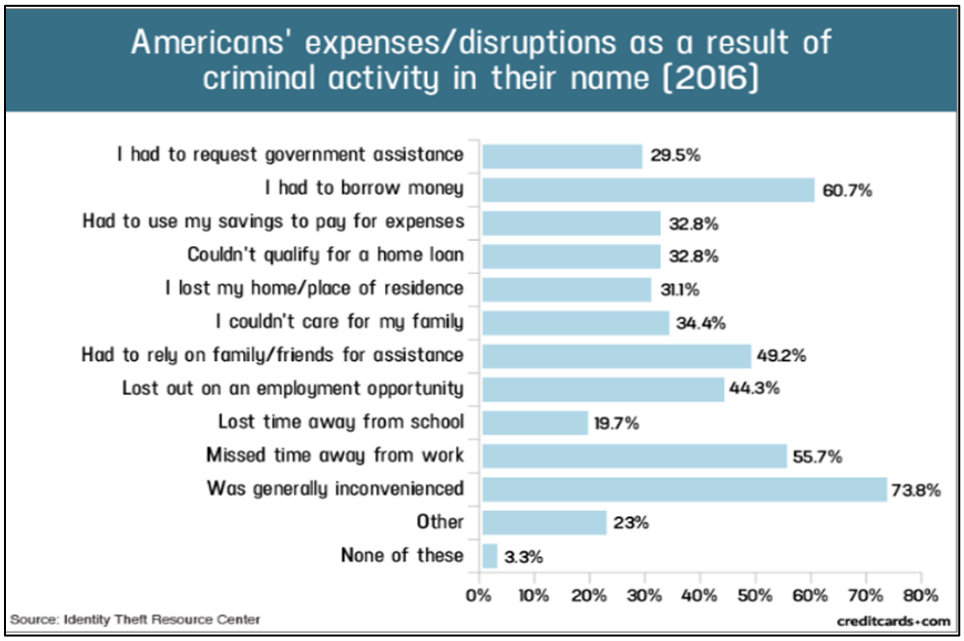
73. A consumer's ability to use their PII is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. Also, a consumer may be unable to open an electronic account where their email address is already associated with another user. In this sense, among others, the theft of PII in the Data Breach led to a diminution in value of the PII.

74. Data breaches, like the one at issue here, damage consumers by interfering with their fiscal autonomy. Any past and potential future misuse of Plaintiff's PII impairs their ability to participate in the economic marketplace.

[9] *See* https://robinhood.com/us/en/support/articles/privacy-policy/ (last visited on Sept. 12, 2023).

[10] *See* John T. Soma, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ('PII') Equals the "Value" of Financial Assets,* 15 Rich. J. L. & Tech. 11, 14 (2009).

75. A study by the Identity Theft Resource Center[11] shows the multitude of harms caused by fraudulent use of PII:



76. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or personal financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[12]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

[11] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Sept. 12, 2023).

[12] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Sept. 12, 2023).

77. PII is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

78. As a result, Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

G. Plaintiff Sergei Stadnik and Class Members' Damages

79. Plaintiff and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

80. Plaintiff and Class Members entrusted their Private Information to Defendant in order to receive Defendant's services. In Plaintiff Stadnik's case, he entrusted his Private Information to Defendant through his affiliation with one of Defendant's clients, Bellco Credit Union.

81. Plaintiff's Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate data security practices.

82. As a direct and proximate result of Sovos's actions and omissions, Plaintiff and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

83. Further, as a direct and proximate result of Sovos's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

84. Plaintiff and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information,

since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiff and Class Members.

85. The Private Information maintained by and stolen from Defendant's systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiff and Class Members, which can be and have been used to carry out targeted fraudulent schemes against Plaintiff and Class Members.

86. Additionally, Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their accounts and records for misuse.

87. Finally, Plaintiff and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach. These losses include, but are not limited to, the following:

a. Monitoring for and discovering fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Placing "freezes" and "alerts" with credit reporting agencies;

e. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

f. Contacting financial institutions and closing or modifying financial accounts;

g. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

h. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

i. Closely reviewing and monitoring bank accounts and credit reports for additional unauthorized activity for years to come.

88. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of Sovos, is protected from future additional breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing personal and financial information is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

89. As a direct and proximate result of Sovos's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

90. Plaintiff brings this action individually and on behalf of all other persons similar situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

91. Specifically, Plaintiff proposes the following Nationwide Class (referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

All individuals in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

92. Excluded from the Class are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal

representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

93. Plaintiff reserves the right to modify or amend the definitions of the proposed Nationwide Class and add subclasses before the Court determines whether certification is appropriate.

94. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

95. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of approximately 215,114 individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Sovos's records, Class Members' records, publication notice, self-identification, and other means.

96. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Sovos engaged in the conduct alleged herein;

b. When Sovos learned of the Data Breach;

c. Whether Sovos's response to the Data Breach was adequate;

d. Whether Sovos unlawfully lost or disclosed Plaintiff's and Class Members' Private Information;

e. Whether Sovos failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

f. Whether Sovos's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether Sovos's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Sovos owed a duty to Class Members to safeguard their Private Information;

i. Whether Sovos breached its duty to Class Members to safeguard their Private Information;

j. Whether hackers obtained Class Members' Private Information via the Data Breach;

k. Whether Sovos had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

l. Whether Sovos breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

m. Whether Sovos knew or should have known that its data security systems and monitoring processes were deficient;

n. What damages Plaintiff and Class Members suffered as a result of Sovos's misconduct;

o. Whether Sovos's conduct was negligent;

p. Whether Sovos's conduct was *per se* negligent;

q. Whether Sovos was unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

97. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

98. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

99. Predominance. Sovos has engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Sovos's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

100. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is

superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Sovos. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

101. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Sovos has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

102. Finally, all members of the proposed Class are readily ascertainable. Sovos has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Sovos.

VI. CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(On behalf of Plaintiff and the Nationwide Class)

103. Plaintiff restates and realleges all of the allegations stated above and hereafter as if fully set forth herein.

104. Sovos knowingly collected, came into possession of, and maintained Plaintiff's and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding,

securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

105. Sovos's duty also included a responsibility to implement processes by which it could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

106. Sovos knew or should have known of the risks inherent in collecting the Private Information of Plaintiff and Class Members and the importance of adequate security. Sovos was on notice because, on information and belief, it knew or should have known that it would be an attractive target for cyberattacks.

107. Sovos owed a duty of care to Plaintiff and Class Members whose Private Information was entrusted to it. Sovos's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect its clients' customers' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiff and Class Members pursuant to the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiff and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

108. Sovos's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

109. Sovos's duty also arose because Defendant was bound by industry standards to protect its clients' customers' confidential Private Information.

110. Plaintiff and Class Members were foreseeable victims of any inadequate security practices on the part of Defendant, and Sovos owed them a duty of care to not subject them to an unreasonable risk of harm.

111. Sovos, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' Private Information within its possession.

112. Sovos, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiff and Class Members.

113. Sovos, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

114. Sovos breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA; and

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised.

115. Sovos acted with reckless disregard for the rights of Plaintiff and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that Plaintiff and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

116. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices on the part of Defendant. Plaintiff and Class Members had no ability to protect their Private Information that was in Defendant's possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

117. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that Plaintiff and the Class had entrusted to it.

118. Sovos's breach of duties owed to Plaintiff and Class Members caused Plaintiff's and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

119. Sovos's breaches of duty also caused a substantial, imminent risk to Plaintiff and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

120. As a result of Sovos's negligence in breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

121. As a direct and proximate result of Sovos's negligent conduct, Plaintiff and Class Members have suffered damages as alleged herein and are at imminent risk of further harm. The injury and harm that Plaintiff and Class Members suffered was reasonably foreseeable.

122. Plaintiff and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

123. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Sovos to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of the Plaintiff and the Nationwide Class)

124. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

125. Pursuant to Section 5 of the FTCA, Sovos had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and Class Members.

126. Sovos breached its duties to Plaintiff and Class Members under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

127. Specifically, Sovos breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper

segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

128. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of Sovos's duty in this regard.

129. Sovos also violated the FTCA by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

130. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiff's and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to Sovos's networks, databases, and computers that stored Plaintiff's and Class Members' unencrypted Private Information.

131. Plaintiff and Class Members are within the class of persons that the FTCA are intended to protect and Sovos's failure to comply with both constitutes negligence *per se*.

132. Plaintiff's and Class Members' Private Information constitutes personal property that was stolen due to Sovos's negligence, resulting in harm, injury, and damages to Plaintiff and Class Members.

133. As a direct and proximate result of Sovos's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized

access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

134. As a direct and proximate result of Sovos's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

135. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Sovos to, inter alia, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT III
BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of Plaintiff and the Nationwide Class)

136. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

137. Defendant entered into contracts, written or implied, with its clients to perform services that include, but are not limited to, providing staffing software and other services. Upon information and belief, these contracts are virtually identical between and among Defendant and its clients around the country whose customers, including Plaintiff and Class Members, were affected by the Data Breach.

138. In exchange, Defendant agreed, in part, to implement adequate security measures to safeguard the PII of Plaintiff and the Class.

139. These contracts were made expressly for the benefit of Plaintiff and the Class, as Plaintiff and Class Members were the intended third-party beneficiaries of the contracts entered

into between Defendant and its clients. Defendant knew that if it were to breach these contracts with its clients, the clients' customers—Plaintiff and Class Members—would be harmed.

140. Defendant breached the contracts it entered into with its clients by, among other things, failing to (i) use reasonable data security measures, (ii) implement adequate protocols and employee training sufficient to protect Plaintiff's Private Information from unauthorized disclosure to third parties, and (iii) promptly and adequately detecting the Data Breach and notifying Plaintiff and Class Members thereof.

141. Plaintiff and the Class were harmed by Defendant's breach of its contracts with its clients, as such breach is alleged herein, and are entitled to the losses and damages they have sustained as a direct and proximate result thereof.

142. Plaintiff and Class Members are also entitled to their costs and attorney's fees incurred in this action.

COUNT IV
UNJUST ENRICHMENT
(On behalf of Plaintiff and the Nationwide Class)

143. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

144. This Count is pleaded in the alternative to Count III above.

145. Plaintiff and Class Members conferred a benefit on Sovos by turning over their Private Information to Defendant and utilizing its services directly or indirectly through their respective employers to whom Plaintiff and Class Members entrusted their Private Information and who subsequently transmitted such Private Information to Defendant.

146. As a result of Plaintiff's and Class Members use of Defendant's services as set forth herein, Defendant received monetary benefits and the use of the valuable Private Information entrusted to it for business purposes and financial gain.

147. Defendant collected, maintained, and stored the Private Information of Plaintiff and Class Members and, as such, had direct knowledge of the monetary benefits conferred upon it (including the use of the valuable Private Information for business purposes and financial gain) by the entities that collected Plaintiff's and Class Members' Private Information and that used Defendant's services.

148. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with the entities that collected Plaintiff's and Class Members' Private Information, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on reasonable data privacy and security measures to secure Plaintiff's and Class Members' Private Information.

149. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Private Information, Defendant, upon information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class Members.

150. If Plaintiff and Class Members had known that Sovos would not adequately secure their Private Information, they would not have agreed to provide such Private Information to Defendant.

151. Due to Sovos's conduct alleged herein, it would be unjust and inequitable under the circumstances for Sovos to be permitted to retain the benefit of its wrongful conduct.

152. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and/or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the

compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in Sovos's possession and is subject to further unauthorized disclosures so long as Sovos fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

153. Plaintiff and Class Members are entitled to full refunds, restitution, and/or damages from Sovos and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by Sovos from its wrongful conduct. This can be accomplished by establishing a constructive trust from which Plaintiff and Class Members may seek restitution or compensation.

154. Plaintiff and Class Members may not have an adequate remedy at law against Sovos, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
DECLARATORY JUDGMENT
(On behalf of Plaintiff and the Nationwide Class)

155. Plaintiff restates and realleges the allegations in the preceding paragraphs as if fully set forth herein.

156. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant

further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the FTCA as described in this Complaint.

157. Sovos owes a duty of care to Plaintiff and Class Members, which required it to adequately secure Plaintiff's and Class Members' Private Information.

158. Sovos still possesses Private Information pertaining to Plaintiff and Class Members.

159. Plaintiff alleges that Sovos's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of his Private Information and the risk remains that further compromises of his Private Information will occur in the future.

160. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Sovos owes a legal duty to secure its clients' customers' Private Information under the common law and Section 5 of the FTCA;

b. Sovos's existing data security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect its clients' customers' Private Information; and

c. Sovos continues to breach this legal duty by failing to employ reasonable measures to secure its clients' customers' Private Information.

161. This Court should also issue corresponding prospective injunctive relief requiring Sovos to employ adequate security protocols consistent with legal and industry standards to protect its clients' customers' Private Information, including the following:

a. Order Sovos to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Sovos must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Sovos's systems on a periodic basis, and ordering Sovos to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Sovos's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its clients' customers about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

162. If an injunction is not issued, Plaintiff will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Sovos. The risk of another such breach is real, immediate, and substantial. If another breach at Sovos occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

163. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Sovos if an injunction is issued. Plaintiff will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Sovos's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Sovos has a pre-existing legal obligation to employ such measures.

164. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Sovos, thus preventing future injury to Plaintiff and others whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above, seeks the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiff and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing Sovos to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members;

e. An order requiring Sovos to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiff and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all triable issues.

DATED: September 13, 2023

Respectfully submitted,

/s/ Christina Xenides

Christina Xenides (Bar No. 677603)
SIRI & GLIMSTAD LLP
1005 Congress Avenue, Suite 925-C36
Austin, TX 78701
Tel: (512) 265-5622
E: cxenides@sirillp.com

Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
745 Fifth Avenue, Suite 500
New York, New York 10151

Tel: (212) 532-1091
E: mbarney@sirillp.com
E: tbean@sirillp.com